Finite Fields and Their Applications 18 (2012) 781–790

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Two classes of permutation polynomials over finite fields

Zhengbang Zha [a,b,*], Lei Hu [b]

[a] School of Mathematical Sciences, Luoyang Normal University, Luoyang 471022, China
[b] State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100049, China

ARTICLE INFO

Article history:
Received 27 August 2011
Revised 15 February 2012
Accepted 20 February 2012
Available online 3 March 2012
Communicated by Rudolf Lidl

MSC:
05A05
11T06

Keywords:
Permutation polynomial
Finite field
Piecewise function

ABSTRACT

Two classes of permutation polynomials over finite fields are presented. The first class is a further study of permutation polynomials of the form $(x^{p^k} - x + \delta)^s + L(x)$ and the second class is a supplement of the recent work of Hou on permutation polynomials. We show the permutation properties of two polynomials in the first class and five polynomials in the second class by using their implicit or explicit piecewise function characteristic over the subsets of the finite field defined by multiplicative or additive characters of the field. Two polynomials in the first class theoretically explain two numerical observations of J. Yuan et al. in their permutation polynomial search experiment.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of a prime power order q. A polynomial $f(x)$ in $\mathbb{F}_q[x]$ is called a permutation polynomial (PP) over $\mathbb{F}_q$ if it induces a one-to-one map from $\mathbb{F}_q$ to itself. PPs have been studied extensively and have important applications in coding theory, cryptography, combinatorics, design theory and so on [4,10–12]. In the recent years, there has been significant progress in finding new permutation polynomials [2,3,5,7].

In [6], Helleseth and Zinoviev derived new identities on Kloosterman sums over $\mathbb{F}_{2^m}$ by making use of PPs of the form $(\frac{1}{x^2+x+\delta})^s + x$. The link between Kloosterman sums and PPs was investigated by J. Yuan et al. in [13,14], and in theses works, many PPs of the form $(x^p - x + \delta)^s + L(x)$ with linearized polynomials $L(x)$ were first introduced and some numerical results on PPs were given. Several of these numerical results can be explained by the new introduced classes of PPs, whilst some

* Corresponding author at: School of Mathematical Sciences, Luoyang Normal University, Luoyang 471022, China.
E-mail addresses: zzb322@yahoo.com.cn (Z. Zha), hu@is.ac.cn (L. Hu).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2012.02.003

remaining unexplained ones are still open. An extension of the above works and two new classes of PPs defined over fields of characteristic 2 were found in [16]. Very recently, P. Yuan and C. Ding [15] gave a unified treatment of some earlier constructions of PPs and get many new specific PPs by using a powerful lemma proved by Akbary, Ghioca and Wang [1].

The concept of reversed Dickson polynomial $D_n(a,x)$ was first defined by Hou, Mullen, Sellers and Yucas in [9] by reversing the roles of the variable and the parameter in the Dickson polynomial $D_n(x,a)$. When $a\neq 0$, $D_n(a,x)$ is a PP over $\mathbb{F}_q$ if and only if $D_n(1,x)$ is a PP over $\mathbb{F}_q$, and the latter is characterized by the functional equation $D_n(1,y(1-y))=y^n+(1-y)^n$. A big problem on reversed Dickson polynomials is to determine for which pairs (q,n) the polynomial $D_n(1,x)$ is a PP over $\mathbb{F}_q$. In the same paper [9], a relation between reversed Dickson permutation polynomials (RDPPs) and almost perfect nonlinear functions was shown and several families of nontrivial RDPPs were presented. A consequent work [8] further presented two new classes of PPs, one of which answered an open question about RDPPs.

In this paper, we present two classes of permutation polynomials which are studied along with the above two directions but are inherently considered to have some piecewise function characteristic for the ease of the proofs of their permutation property. The first class we present is a further study of permutation polynomials of the form $(x^{p^k}-x+\delta)^s+L(x)$, where p is the characteristic of the field. Two of them theoretically explain two numerical observation of J. Yuan et al. in their permutation polynomial search experiment, which can be seen in Section 2. The second class is a supplement of the recent work of Hou on permutation polynomials and the polynomials presented in the class have explicit piecewise function characteristic, we discuss them in Section 3.

2. Permutation polynomials of the form $(x^{p^k}-x+\delta)^s+L(x)$

Let p be an odd prime and n be a positive integer. The quadratic character χ on $\mathbb{F}_{p^n}$ is defined by $\chi(0)=0$, $\chi(x)=1$ if x is a square in $\mathbb{F}_{p^n}\backslash\{0\}$ and $\chi(x)=-1$ if x is a nonsquare in $\mathbb{F}_{p^n}\backslash\{0\}$.

The trace function from $\mathbb{F}_{p^n}$ onto its subfield $\mathbb{F}_{p^k}$ is defined as

$$\mathrm{Tr}_{n/k}(x)=x+x^{p^k}+x^{p^{2k}}+\cdots+x^{p^{n-k}}.$$

The absolute trace function (i.e., for $k=1$) is simply denoted by Tr (for fixed n) and is then defined by $\mathrm{Tr}(x)=x+x^p+x^{p^2}+\cdots+x^{p^{n-1}}$. Clearly, if $y\in\mathbb{F}_{p^n}$ and $\mathrm{Tr}_{n/k}(y)=0$ then $\mathrm{Tr}(y)=\mathrm{Tr}_{k/1}(\mathrm{Tr}_{n/k}(y))=\mathrm{Tr}(0)=0$, and hence the set $\{x\in\mathbb{F}_{p^n}\mid \mathrm{Tr}_{n/k}(x)\neq 0\}$ is a larger subset of $\mathbb{F}_{p^n}$ which includes $\{x\in\mathbb{F}_{p^n}\mid \mathrm{Tr}(x)\neq 0\}$ as its subset.

Theorem 1. *Let p be an odd prime, n,k be positive integers and $d=\gcd(n,k)$. Let $\delta\in\mathbb{F}_{p^n}$ with $\mathrm{Tr}_{n/d}(\delta)\neq 0$. Then $(x^{p^k}-x+\delta)^{\frac{p^n+1}{2}}+x^{p^k}+x$ is a PP over $\mathbb{F}_{p^n}$.*

Proof. First note that $x^{p^k}-x+\delta\neq 0$ and $\chi(x^{p^k}-x+\delta)\neq 0$ for any $x\in\mathbb{F}_{p^n}$ since $\mathrm{Tr}_{n/d}(\delta)\neq 0$. Similarly, for any $b\in\mathbb{F}_{p^n}$, $b^{p^k}-b+\delta^{p^k}+\delta\neq 0$ since $\mathrm{Tr}_{n/d}(\delta^{p^k}+\delta)=2\,\mathrm{Tr}_{n/d}(\delta)\neq 0$. It suffices to prove that the equation

$$\left(x^{p^k}-x+\delta\right)^{\frac{p^n+1}{2}}+x^{p^k}+x=b \tag{1}$$

has at most one solution. Let x be such a solution. It belongs to either $D_1=\{a\in\mathbb{F}_{p^n}\mid \chi(a^{p^k}-a+\delta)=1\}$ or $D_{-1}=\{a\in\mathbb{F}_{p^n}\mid \chi(a^{p^k}-a+\delta)=-1\}$.

If $x\in D_1$, then we get $2x^{p^k}=b-\delta$ from Eq. (1). We have $x^{p^k}=\frac{b-\delta}{2}$ and $x^{p^k}-x+\delta=\frac{1}{2}(b-b^{p^{n-k}}+\delta+\delta^{p^{n-k}})$. Since $\frac{1}{2}(b^{p^k}-b+\delta^{p^k}+\delta)=(\frac{1}{2}(b-b^{p^{n-k}}+\delta+\delta^{p^{n-k}}))^{p^k}$, we get $\chi(\frac{1}{2}(b^{p^k}-b+\delta^{p^k}+\delta))=\chi(\frac{1}{2}(b-b^{p^{n-k}}+\delta+\delta^{p^{n-k}}))=1$.

If $x \in D_{-1}$, then we get $2x = b + \delta$ from Eq. (1). We have $x = \frac{b+\delta}{2}$ and $x^{p^k} - x + \delta = \frac{1}{2}(b^{p^k} - b + \delta^{p^k} + \delta)$. In this case, we must have $\chi(\frac{1}{2}(b^{p^k} - b + \delta^{p^k} + \delta)) = -1$.

From the above discussion, we conclude that: if $\chi(\frac{1}{2}(b^{p^k} - b + \delta^{p^k} + \delta)) = 1$, then there exists no solution in D_{-1} of Eq. (1) and the unique possible solution is in D_1. Similarly, if $\chi(\frac{1}{2}(b^{p^{2k}} - b + \delta^{p^k} + \delta)) = -1$, then the unique solution is in D_{-1}. Thus, for any fixed b, there is at most one solution for the equation $f(x) = b$. □

Remark 1. The permutation polynomial given in Theorem 1 has a simple implicit piecewise function expression, that is, when the variable x takes values in the domain D_1 or D_{-1}, the expression of the function become a linearized one.

To derive a permutation polynomial of the form $(x^{p^k} - x + \delta)^s + x$ from the PP presented in Theorem 1, we make a replacement of variable x by y such that $y = x + x^{p^k}$. To this goal, we use the following trivial fact.

Lemma 1. *Let $d = \gcd(n, k)$. Consider polynomials over a finite field of odd characteristic p.*

(i) $\gcd(x^k + 1, x^n - 1) = 1$ *if and only if n/d is odd (or equivalently, the largest factor of n of the form of power of 2 divides that of k).*
(ii) $x + x^{p^k}$ *is a PP over $\mathbb{F}_{p^n}$ if and only if $\gcd(x^k + 1, x^n - 1) = 1$, or namely if and only if n/d is odd.*

In the case that n/d is odd, if we make the replacement of variable x by y such that $y = x + x^{p^k}$, then we have $x = \frac{1}{2}\sum_{i=0}^{(n/d)-1}(-1)^i y^{p^{ik}}$, and $x^{p^k} - x = \sum_{i=1}^{(n/d)-1}(-1)^{i+1} y^{p^{ik}}$. Further, if we assume $n = 3d$, then we have $x^{p^k} - x = y^{p^k} - y^{p^{2k}}$, and the permutation polynomial in Theorem 1 become

$$\left(y^{p^k} - y^{p^{2k}} + \delta\right)^{\frac{p^n-1}{2}+1} + y = \left(y^{p^{2k}} - y + \delta^{p^{-2k}}\right)^{\frac{p^n-1}{2}+p^{2k}} + y.$$

This deduces the following consequence.

Corollary 1. *Let p be an odd prime, $n = 3d$, $k = d$ or $2d$, and $\delta \in \mathbb{F}_{p^n}$ with $\mathrm{Tr}_{n/d}(\delta) \neq 0$. Then $(x^{p^k} - x + \delta)^{\frac{p^n-1}{2}+p^k} + x$ is a PP over $\mathbb{F}_{p^n}$.*

From Corollary 1, we get that $(x^3 - x + \delta)^{16} + x$ with $\mathrm{Tr}(\delta) \neq 0$ permutes $\mathbb{F}_{3^3}$, which explains one experimental observation in [14].

To remove the condition of $\mathrm{Tr}_{n/d}(\delta) \neq 0$ in Theorem 1 and Corollary 1, we consider permutation polynomials over fields of characteristic 3, and we have the following theorem.

Theorem 2. *Let $n = 3d$, $k = d$ or $2d$, and $\delta \in \mathbb{F}_{3^d}$. Then $(x^{3^k} - x + \delta)^{\frac{3^n-1}{2}+3^{ik}} + x$ is a PP over $\mathbb{F}_{3^n}$ for any $i = 0$, 1 or 2.*

Proof. The proof for different i is similar, below we give the proof for $i = 1$. We prove that the equation $(x^{3^k} - x + \delta)^{\frac{3^n-1}{2}+3^k} + x = b$ has exactly one solution for any $b \in \mathbb{F}_{3^n}$. Similarly as in the proof of Theorem 1, we let x be such a solution, and it belongs to $D_0 = \{a \in \mathbb{F}_{3^n} \mid a^{3^k} - a + \delta = 0\}$, $D_1 = \{a \in \mathbb{F}_{3^n} \mid \chi(a^{3^k} - a + \delta) = 1\}$, or $D_{-1} = \{a \in \mathbb{F}_{3^n} \mid \chi(a^{3^k} - a + \delta) = -1\}$.

If $x \in D_0$, then from the equation $(x^{3^k} - x + \delta)^{\frac{3^n-1}{2}+3^k} + x = b$ we get $x = b$ and $b^{3^k} - b + \delta = 0$.

If $x \in D_1$, then we get $(x^{3^k} - x + \delta)^{3^k} + x = b$. That is, $x^{3^{2k}} - x^{3^k} + \delta + x = b$ since $\delta \in \mathbb{F}_{3^d}$. Adding this equation with its 3^kth power, we have $2x + 2\delta = b^{3^k} + b$, $x = -\delta - b^{3^k} - b$, and hence, $x^{3^k} - x + \delta = b - b^{3^{2k}} + \delta = (b^{3^k} - b + \delta)^{3^{2k}}$. The latter leads to $\chi(b^{3^k} - b + \delta) = \chi(x^{3^k} - x + \delta) = 1$.

If $x \in D_{-1}$, then we get $-(x^{3^k}-x+\delta)^{3^k}+x=b$ and $-x^{3^{2k}}+x^{3^k}-\delta+x=b$. Similarly as in the above paragraph, adding the latter equation with its 3^kth power, we have $2x^{3^k}-2\delta=b^{3^k}+b$, $x=\delta-b^{3^{2k}}-b$, and $x^{3^k}-x+\delta=b^{3^{2k}}-b^{3^k}+\delta=(b^{3^k}-b+\delta)^{3^k}$. The latter leads to $\chi(b^{3^k}-b+\delta)=\chi(x^{3^k}-x+\delta)=-1$.

The above discussion says that the equation $(x^{3^k}-x+\delta)^{\frac{3^n-1}{2}+3^k}+x=b$ has solutions in only one domain D_j to which b belongs, where $j=0$, 1, or -1, and there exists exactly one solution. This proves the theorem. □

The following trivial lemma presents a permutation over a finite field according to its piecewise property on the domains $T_i=\{x\in\mathbb{F}_{p^n} \mid \mathrm{Tr}(x)=i\}$, $i=0,1,\ldots,p-1$.

Lemma 2. *Let $\{h_0,h_1,\ldots,h_{p-1}\}$ be a permutation on $\{0,1,\ldots,p-1\}$. A mapping defined on $\mathbb{F}_{p^n}$ which one-to-one maps T_i to T_{h_i} for any $i=0,1,\ldots,p-1$ is a permutation over $\mathbb{F}_{p^n}$.*

The following two lemmas are needed in the sequel.

Lemma 3. *The polynomial $x^{p^k}-x$ has no nonzero root in T_0 if and only if $\gcd(n,k)=1$ and $n\not\equiv 0 \pmod p$.*

Proof. The nonzero roots of $x^{p^k}-x$ are (p^k-1)th roots of unity. They are also (p^n-1)th roots of unity and since $\gcd(p^n-1,p^k-1)=p^d-1$, they are hence (p^d-1)th roots of unity, where $d=\gcd(k,n)$. Thus, the roots of $x^{p^k}-x$ form the subfield $\mathbb{F}_{p^d}$. If $d>1$, there is a nonzero element θ of $\mathbb{F}_{p^d}$ such that $\mathrm{Tr}_{d/1}(\theta)=0$ and hence, $\mathrm{Tr}_{n/1}(\theta)=\mathrm{Tr}_{d/1}(\mathrm{Tr}_{n/d}(\theta))=\frac{n}{d}\mathrm{Tr}_{d/1}(\theta)=0$. If $d=1$, then for any $0\neq\theta\in\mathbb{F}_p$, $\mathrm{Tr}_{n/1}(\theta)=n\theta\neq 0$ if and only if $n\not\equiv 0 \pmod p$. □

Lemma 4. *Let n, k be integers and p be an odd prime. If $\gcd(\frac{n}{\gcd(n,k)},p-1)=1$, then $\frac{\rho-1}{\rho}$ is not a (p^k-1)th power over $\mathbb{F}_{p^n}$ for any $\rho\in\mathbb{F}_p$ and $\rho\neq 0,1$.*

Proof. For all $\rho\in\mathbb{F}_p$ with $\rho\neq 0,1$, the expression $c=\frac{\rho-1}{\rho}$ takes exactly all elements in $\mathbb{F}_p\setminus\{0,1\}$. Let $k'=\gcd(n,k)$. Then $\gcd(p^k-1,p^n-1)=p^{k'}-1$, and the all (p^k-1)th powers in $\mathbb{F}_{p^n}$ are exactly the $(p^{k'}-1)$th powers in $\mathbb{F}_{p^n}$. Thus, the condition that $c\in\mathbb{F}_p\setminus\{0,1\}$ is not a (p^k-1)th power in $\mathbb{F}_{p^n}$ is equivalent to that $c^{\frac{p^n-1}{p^{k'}-1}}\neq 1$. Let $u=n/k'$, using that $c^p\equiv c \pmod p$, we have

$$c^{\frac{p^n-1}{p^{k'}-1}}=cc^{p^{k'}}c^{p^{2k'}}\cdots c^{p^{k'(u-1)}}\equiv c^u \pmod p.$$

Thus the desired claim is to say that $c^u\neq 1$ or equivalently, $c^{\gcd(u,p-1)}\neq 1$. Now the requirement that $c^{\gcd(u,p-1)}\neq 1$ holds for all $c\in\mathbb{F}_p\setminus\{0,1\}$ is exactly to say $\gcd(u,p-1)=1$. □

Using Lemma 2, we try to find permutation polynomials among ones of the form

$$f(x)=\left(x^{p^k}-x+\delta\right)+ax+b\,\mathrm{Tr}(x)+cx\,\mathrm{Tr}(x) \tag{2}$$

and

$$\mathrm{Tr}(x)\left(x^{p^k}-x+\delta\right)+ax+b\,\mathrm{Tr}(x)+cx\,\mathrm{Tr}(x), \tag{3}$$

where $a,b,c\in\mathbb{F}_p$. For the function defined by (2), when $x\in T_i$,

$$f(x)=x^{p^k}+(a+ci-1)x+bi+\delta,\qquad \mathrm{Tr}\big(f(x)\big)=ci^2+(a+bn)i+\mathrm{Tr}(\delta).$$

The requirement that $ci^2 + (a + bn)i + \mathrm{Tr}(\delta)$ is a permutation on $\{0, 1, \ldots, p-1\}$ is equivalent to say that $c = 0$ and $a + bn \neq 0$ for odd p and $a + bn + c = 1$ for $p = 2$.

Firstly, we consider the case that p is odd and $c = 0$. When $a = 0$, from Lemma 3 we get that $f(x) = x^{p^k} - x + bi + \delta$ is injective from T_i to $\mathbb{F}_{p^n}$ under the conditions $n \not\equiv 0 \pmod p$ and $\gcd(n, k) = 1$. When $a = 1$, $f(x) = x^{p^k} + bi + \delta$ is a PP on the whole field. Utilizing Lemma 4, we can show $1 - a = \frac{a^{-1}-1}{a^{-1}}$ is not a $(p^k - 1)$th power over $\mathbb{F}_{p^n}$ for any $a \neq 0, 1$ under the condition of Lemma 4. This leads to $f(x)$ is a PP over $\mathbb{F}_{p^n}$ for any $a \neq 0, 1$ under the condition $\gcd(\frac{n}{\gcd(n,k)}, p - 1) = 1$.

Similar discussion is done for the polynomial of the form (3) and for the case $p = 2$. This leads to the following theorem.

Theorem 3. (i) *Let p be an odd prime and $a, b \in \mathbb{F}_p$. Then*

$$f(x) = \left(x^{p^k} - x + \delta\right) + ax + b\,\mathrm{Tr}(x)$$

is a PP over $\mathbb{F}_{p^n}$ if $a + bn \neq 0 \in \mathbb{F}_p$ and one of the following conditions holds: (1) $a = 0$, $n \not\equiv 0 \pmod p$, *and* $\gcd(n, k) = 1$. (2) $a = 1$. (3) $a \neq 0$, $a \neq 1$, *and* $\gcd(\frac{n}{\gcd(n,k)}, p - 1) = 1$.

$$\mathrm{Tr}(x)\left(x^{p^k} - x + \delta\right) + x + b\,\mathrm{Tr}(x)$$

is a PP over $\mathbb{F}_{p^n}$ if $bn + \mathrm{Tr}(\delta) \neq -1$ and $\gcd(\frac{n}{\gcd(n,k)}, p - 1) = 1$.

(ii) *Let $a, b, c \in \mathbb{F}_2$. Then*

$$\left(x^{2^k} + x + \delta\right) + ax + b\,\mathrm{Tr}(x) + cx\,\mathrm{Tr}(x)$$

is a PP over $\mathbb{F}_{2^n}$ if and only if $(a, c, bn) = (1, 0, 0)$, or $(a, c) \neq (1, 0)$ and $a + b + c = 1$ and $\gcd(n, k) = 1$ and n is odd.

$$\mathrm{Tr}(x)\left(x^{2^k} + x + \delta\right) + x + b\,\mathrm{Tr}(x) + cx\,\mathrm{Tr}(x)$$

is a PP over $\mathbb{F}_{2^n}$ if and only if $c = 0$ and $\mathrm{Tr}(\delta) = nb$, or $c = 1$, $\mathrm{Tr}(\delta) + b = 1$, $\gcd(n, k) = 1$ and n is odd.

Note that Theorem 3 gives some explicit PPs of Corollaries 3.4 and 3.5 in [15].

Inspired by the idea of Theorem 6.4 in [15], we get the following theorems.

Theorem 4. *Let t be an even integer and $n = 2k$. Let $\beta, \gamma \in \mathbb{F}_{p^k}$, $\gamma \neq 0$, $\delta \in \mathbb{F}_{p^n}$, $\delta^{p^k} = -\delta$, and $\mathrm{Tr}(\beta\gamma^{-1}) \neq -1$. Then $f(x) = (x^{p^k} - x + \delta)^t + \gamma x + \beta\,\mathrm{Tr}(x)$ is a PP over $\mathbb{F}_{p^n}$.*

Proof. Assume there exist $x, a \in \mathbb{F}_{p^n}$ such that $f(x) = f(x + a)$. Then we have

$$\left(x^{p^k} - x + \delta + a^{p^k} - a\right)^t - \left(x^{p^k} - x + \delta\right)^t = -\gamma a - \beta\,\mathrm{Tr}(a). \tag{4}$$

Taking Eq. (4) to the p^kth powers, we obtain

$$\left(x^{p^k} - x + \delta + a^{p^k} - a\right)^t - \left(x^{p^k} - x + \delta\right)^t = -\gamma^{p^k} a^{p^k} - \beta^{p^k}\,\mathrm{Tr}(a) \tag{5}$$

since $\delta^{p^k} = -\delta$ and t is even. From Eqs. (4) and (5), we obtain $\gamma a + \beta\,\mathrm{Tr}(a) = \gamma^{p^k} a^{p^k} + \beta^{p^k}\,\mathrm{Tr}(a)$. Since $\beta = \beta^{p^k}$ and $\gamma = \gamma^{p^k} \neq 0$, then we get $a = a^{p^k}$. Substituting it into Eq. (4), we have $\gamma a + \beta\,\mathrm{Tr}(a) = 0$. Then we have $a = -\beta\gamma^{-1}\,\mathrm{Tr}(a)$ and $\mathrm{Tr}(a) = -\mathrm{Tr}(\beta\gamma^{-1})\,\mathrm{Tr}(a)$. It leads to $a = \mathrm{Tr}(a) = 0$

from the assumption $\mathrm{Tr}(\beta\gamma^{-1}) \neq -1$. Then we get that $f(x) = (x^{p^k} - x + \delta)^t + \gamma x + \beta \mathrm{Tr}(x)$ is a PP over $\mathbb{F}_{p^n}$. □

Similarly to the proof of Theorem 4, we can prove the following theorem.

Theorem 5. *Let t be any integer and $n = 2k$. Let $\delta, \beta \in \mathbb{F}_{p^k}$, $\gamma \in \mathbb{F}_{p^n}$, $\gamma = -\gamma^{p^k} \neq 0$. Then $f(x) = (x^{p^k} + x + \delta)^t + \gamma x + \beta \mathrm{Tr}(x)$ is a PP over $\mathbb{F}_{p^n}$.*

Remark 2. The absolute trace term $\beta \mathrm{Tr}(x)$ in the expressions of the PPs given in Theorems 4 and 5 can be replaced by the relative trace term $\beta \mathrm{Tr}_{n/k}(x)$, and the corresponding requirement $\mathrm{Tr}(\beta\gamma^{-1}) \neq -1$ turns to $\mathrm{Tr}_{n/k}(\beta\gamma^{-1}) \neq -1$. Since $\mathrm{Tr}_{n/k}(\beta\gamma^{-1}) = \mathrm{Tr}(\beta\gamma^{-1}) = 0$ in Theorem 5, this requirement is equivalent to $2\beta \neq -\gamma$ for Theorem 4 and automatically holds for Theorem 5. We note that PPs of the form $(x^{p^k} - x + \delta)^t + \gamma x + \beta \mathrm{Tr}_{n/k}(x)$ are presented in the investigation of Theorem 6.4 in [15]. In Theorems 4 and 5, we get some new PPs just by replacing the relative trace term $\beta \mathrm{Tr}_{n/k}(x)$ with the absolute trace term $\beta \mathrm{Tr}(x)$. The new PPs can also be proved by using the powerful Lemma 2.4 in [15].

Remark 3. The permutation property of $(x^{p^k} + x + \delta)^t + \gamma x + \beta \mathrm{Tr}_{n/k}(x)$ in the case of $p = 2$ can also be proved by using a similar idea of Lemma 2. If $\mathrm{Tr}_{n/k}(x) = i$, we get $f(x) = g_i(x) := (x^{2^k} + x + \delta)^t + \gamma x + \beta i$ and $\mathrm{Tr}_{n/k}(g_i(x)) = \gamma i$. Since $\delta, \gamma \in \mathbb{F}_{2^k}$ and $\gamma \neq 0$, we can first show that $(x^{2^k} + x + \delta)^t + \gamma x$ is a PP over $\mathbb{F}_{2^n}$. Then $g_i(x)$ is injective on $\mathbb{F}_{2^n}$, and $\mathrm{Tr}(g_i(x)) \neq \mathrm{Tr}(g_j(x))$ for $i \neq j \in \mathbb{F}_{2^k}$ since $\gamma \neq 0$.

Theorem 6. *Let $n = 4k$ and δ be an element of $\mathbb{F}_{p^n}$ with $\mathrm{Tr}_{n/k}(\delta) \neq -1$. Then $f(x) = (x^{p^k} - x + \delta)^{p^k(p^{2k}+1)} + x$ is a PP over $\mathbb{F}_{p^n}$.*

Proof. It suffices to prove that the equation

$$\left(x^{p^k} - x + \delta\right)^{p^k(p^{2k}+1)} + x = b \tag{6}$$

has at most one solution for each $b \in \mathbb{F}_{p^n}$.

Case I: If $x^{p^k} - x + \delta = 0$, then we get $x = b$ and $b^{p^k} - b + \delta = 0$.

Case II: If $x^{p^k} - x + \delta \neq 0$, then we get $b - x \neq 0$. From Eq. (6), we have $(b - x)^{p^{2k}-1} = 1$, which leads to

$$x^{p^{2k}} - x + b - b^{p^{2k}} = 0. \tag{7}$$

Let $y = x^{p^k} - x + \delta$ and $\theta = b^{p^{2k}} - b + \delta + \delta^{p^k}$. Then we get $y^{p^k} + y = x^{p^{2k}} - x + \delta^{p^k} + \delta = \theta$ by Eq. (7). Now we get

$$y^{p^k} = -y + \theta, \qquad y^{p^{2k}} = -y^{p^k} + \theta^{p^k} = y - \theta + \theta^{p^k}, \qquad y^{p^{3k}} = -y + \theta - \theta^{p^k} + \theta^{p^{2k}}.$$

By Eq. (6), $x = b - y^{p^{3k}+p^k}$, from which together with $y = x^{p^k} - x + \delta$ we get

$$y = b^{p^k} - y^{1+p^{2k}} - b + y^{p^{3k}+p^k} + \delta. \tag{8}$$

Substituting the values of y^{p^k}, $y^{p^{2k}}$ and $y^{p^{3k}}$ into Eq. (8), we get

$$\left(1 + \theta + \theta^{p^{2k}}\right) y = b^{p^k} - b + \delta + \theta\left(\theta - \theta^{p^k} + \theta^{p^{2k}}\right). \tag{9}$$

Since

$$1+\theta+\theta^{p^{2k}}=1+b^{p^{2k}}-b+\delta+\delta^{p^k}+b-b^{p^{2k}}+\delta^{p^{2k}}+\delta^{p^{3k}}=1+\mathrm{Tr}_{n/k}(\delta)$$

and $\mathrm{Tr}_{n/k}(\delta)\neq -1$, we get $1+\theta+\theta^{p^{2k}}\neq 0$. Therefore, we get only one solution y from Eq. (9). This leads to only one solution x since $x=b-y^{p^{3k}+p^k}$.

When $b^{p^k}-b+\delta\neq 0$, the unique possible solution of Eq. (6) is in Case II. And when $b^{p^k}-b+\delta=0$, we get $b^{p^k}=b-\delta$ and $b^{p^{2k}}=b^{p^k}-\delta^{p^k}=b-\delta-\delta^{p^k}$. In Case I, we have one solution $x=b$. In Case II, we have $\theta=b^{p^{2k}}-b+\delta+\delta^{p^k}=0$ and $y=0$ from Eq. (9). This leads to one solution $x=b-y^{p^{3k}+p^k}=b$, which contradicts to the first assumption $x^{p^k}-x+\delta\neq 0$. Therefore, we get only one solution $x=b$ of Eq. (6) in Case I when $b^{p^k}-b+\delta=0$. The proof is completed. □

By Theorem 6, we get that $(x^3-x+\delta)^{30}+x$ with $\mathrm{Tr}(\delta)=1$ permutes $\mathbb{F}_{3^4}$, which explains another experimental observation in [14].

3. Permutation polynomials with explicit piecewise function forms

This section presents several PPs with explicit piecewise function forms; they are motivated by the recent work of Hou on permutation polynomials [8]. A concrete result of his study is the following theorem.

Theorem 7. *(See [8, Theorem 1.1].) Let e be a positive even integer. Then $f(x)=(1-x-x^2)x^{\frac{3^e+1}{2}}-1-x+x^2$ is a PP over $\mathbb{F}_{3^e}$.*

Here we give a slight generalization of this theorem as the following proposition.

Proposition 1. *Let t be a positive integer with $\gcd(t,3^n-1)=1$. Assume $\theta,\beta\in\mathbb{F}_{3^n}$ with $\chi(\theta)=\chi(\beta)=1$. Then $f(x)=(\beta x^3+\beta\theta x^2+\beta\theta^2 x-x^t)x^{\frac{3^n-1}{2}}-(\beta x^3+\beta\theta x^2+\beta\theta^2 x+x^t)$ is a PP over $\mathbb{F}_{3^n}$.*

Proof. By the definition of the quadratic character, we get that

$$f(x)=\begin{cases}0, & \text{if } x=0,\\ x^t, & \text{if } \chi(x)=1,\\ \beta(x^3+\theta x^2+\theta^2 x), & \text{if } \chi(x)=-1.\end{cases}$$

We assume that there exist $x_1,x_2\in\mathbb{F}_{3^n}$ with $x_1\neq x_2$ such that $f(x_1)=f(x_2)$.

Case I. Assume $x_1=0$ and $x_2\neq 0$. If $\chi(x_2)=1$, then $x_2^t=f(x_1)=0$ and $x_2=0$. If $\chi(x_2)=-1$, then $\beta(x_2^3+\theta x_2^2+\theta^2 x_2)=0$, which implies either $x_2=0$ or $x_2=\theta$. The latter will deduce $\chi(x_2)=\chi(\theta)=1$, which is a contradiction.

Case II. Assume $\chi(x_1)=\chi(x_2)=1$. Since $\gcd(t,3^n-1)=1$, then we have $x_1^t=x_2^t$, i.e., $x_1=x_2$, which is a contradiction.

Case III. Assume $\chi(x_1)=\chi(x_2)=-1$. Then we get $\beta(x_1^3+\theta x_1^2+\theta^2 x_1)=\beta(x_2^3+\theta x_2^2+\theta^2 x_2)$. It leads to $(x_1-x_2)(x_1^2+(x_2+\theta)x_1+(x_2-\theta)^2)=0$. Equation $x_1^2+(x_2+\theta)x_1+(x_2-\theta)^2=0$ has a solution $x_1\in\mathbb{F}_{3^n}$ only if $\chi((x_2+\theta)^2-4(x_2-\theta)^2)=\chi(\theta x_2)=1$. Then we obtain $\chi(x_2)=1$, which is a contradiction.

Case IV. Assume $\chi(x_1)=1$ and $\chi(x_2)=-1$. In this case, $f(x_1)=f(x_2)$ implies $x_1^t=\beta x_2(x_2-\theta)^2$. Since $\gcd(t,3^n-1)=1$, we obtain t is odd. Then we get $\chi(x_1)=\chi(x_2)$ by $\chi(\beta)=1$, which is also a contradiction. □

The following theorem presents permutation polynomials over general odd characteristic fields and with similar expressions as that in Theorem 7. The proof is similar as for Proposition 1.

Theorem 8. *Let p be an odd prime and n, t, l be any positive integers. Then $f(x) = (1-x^t)x^{\frac{p^n-1}{2}+l} - x^l - x^{t+l}$ is a PP over $\mathbb{F}_{p^n}$ provided*

(i) $\gcd(l, p^n-1) = 1$ *and* $\gcd(t+l, p^n-1) = 1$; *or*
(ii) $\gcd(l, p^n-1) = 1$, $\gcd(t+l, p^n-1) = 2$ *and* $p^n \equiv 3 \pmod 4$.

Proof. By the definition of the quadratic character, we have

$$f(x) = \begin{cases} 0, & \text{if } x = 0, \\ -2x^{t+l}, & \text{if } \chi(x) = 1, \\ -2x^l, & \text{if } \chi(x) = -1. \end{cases}$$

We assume that there exist $x_1 \neq x_2 \in \mathbb{F}_{p^n}$ such that $f(x_1) = f(x_2)$.

Case I. Assume $x_1 = 0$ and $x_2 \neq 0$. It is obviously impossible.

Case II. Assume $\chi(x_1) = \chi(x_2) = 1$. Then $-2x_1^{t+l} = -2x_2^{t+l}$. If $\gcd(t+l, p^n-1) = 1$, we get $x_1 = x_2$. If $\gcd(t+l, p^n-1) = 2$, then $x_1^2 = x_2^2$ and $x_1 = -x_2$ since $x_1 \neq x_2$. From $p^n \equiv 3 \pmod 4$ and $\chi(-1) = -1$, we get $\chi(x_1) = -\chi(x_2)$, which is a contradiction.

Case III. Assume $\chi(x_1) = \chi(x_2) = -1$. Then we get $-2x_1^l = -2x_2^l$. As $\gcd(l, p^n-1) = 1$, we have $x_1 = x_2$, which is a contradiction.

Case IV. Assume $\chi(x_1) = 1$ and $\chi(x_2) = -1$. In this case, $f(x_1) = f(x_2)$ implies $x_1^{t+l} = x_2^l$. We can deduce that l is odd from $\gcd(l, p^n-1) = 1$. Then we can get $\chi(x_2) = \chi(x_1^{t+l}) = 1$, which is a contradiction. □

Below we consider PPs with piecewise function forms by a power function $\varphi(x)$. The function $\varphi(x)$ is defined over finite fields of size $p^n \equiv 1 \pmod 3$ as $\varphi(x) = x^{\frac{p^n-1}{3}}$. Let ω be an element of $\mathbb{F}_{p^n}$ of order 3, for nonzero $x \in \mathbb{F}_{p^n}$, $\varphi(x)$ equals to 1, ω, or ω^2. Trivially, $\varphi(0) = 0$.

Theorem 9. *Assume $p^n \equiv 1 \pmod 3$. Then*

$$f(x) = x\big(x^{\frac{p^n-1}{3}} - \omega\big)\big(x^{\frac{p^n-1}{3}} - \omega^2\big) + x^3\big(x^{\frac{p^n-1}{3}} - 1\big)\big(x^{\frac{p^n-1}{3}} - \omega^2\big) + \omega x^p\big(x^{\frac{p^n-1}{3}} - 1\big)\big(x^{\frac{p^n-1}{3}} - \omega\big)$$

is a PP over $\mathbb{F}_{p^n}$ if

(i) $p \equiv 1 \pmod 3$ *and* $\frac{p-1}{3}n \equiv 1 \pmod 3$; *or*
(ii) $p \equiv 2 \pmod 3$, *n is even and* $\frac{p+1}{3}n \equiv 1 \pmod 3$.

Proof. Note that when $p \equiv 1 \pmod 3$, the condition $\frac{p-1}{3}n \equiv 1 \pmod 3$ is equivalent to that $p^n \equiv 4 \pmod 9$, and when $p \equiv 2 \pmod 3$, the condition that n is even and $\frac{p+1}{3}n \equiv 1 \pmod 3$ is equivalent to that $p^n \equiv 7 \pmod 9$.

By the definition of $\varphi(x)$, we have

$$f(x) = \begin{cases} 0, & \text{if } x = 0, \\ (1-\omega)(1-\omega^2)x, & \text{if } \varphi(x) = 1, \\ (\omega-1)(\omega-\omega^2)x^3, & \text{if } \varphi(x) = \omega, \\ (1-\omega)(\omega^2-\omega)x^p, & \text{if } \varphi(x) = \omega^2. \end{cases}$$

We assume that there exist $x_1, x_2 \in \mathbb{F}_{p^n}$ with $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$.

Case I. Assume $x_1 = 0$ and $x_2 \neq 0$. It is obviously impossible.

Case II. Assume $\varphi(x_1) = \varphi(x_2) = 1$. In this case, $f(x_1) = f(x_2)$ implies $x_1 = x_2$, which is a contradiction.

Case III. Assume $\varphi(x_1)=\varphi(x_2)=\omega$. Then $x_1^3=x_2^3$. It leads to $x_1=\omega x_2$ or $x_1=\omega^2 x_2$. If $x_1=\omega x_2$, then we can get $x_1^{\frac{p^n-1}{3}}=(\omega x_2)^{\frac{p^n-1}{3}}$ which implies $\omega^{\frac{p^n-1}{3}}=1$. This contradicts to the condition $\frac{p^n-1}{3}\not\equiv 0 \pmod 3$. Similarly, we can show that $x_1=\omega^2 x_2$ does not hold.

Case IV. Assume $\varphi(x_1)=\varphi(x_2)=\omega^2$. From $x_1^p=x_2^p$, we also get $x_1=x_2$, which leads to contradiction.

Case V. Assume $\varphi(x_1)=1$ and $\varphi(x_2)=\omega$. We have $(1-\omega)(1-\omega^2)x_1=(\omega-1)(\omega-\omega^2)x_2^3$, which implies $x_1=\omega^2 x_2^3$. Then we get $\omega^{\frac{2(p^n-1)}{3}}=1$ from $x_1^{\frac{p^n-1}{3}}=\omega^{\frac{2(p^n-1)}{3}}x_2^{p^n-1}$. This is impossible since $\frac{p^n-1}{3}\not\equiv 0 \pmod 3$.

Case VI. Assume $\varphi(x_1)=1$ and $\varphi(x_2)=\omega^2$. Similarly to the discussion in Case V, we get $x_1=\omega^2 x_2^p$, which implies $1=\omega^{2(\frac{p^n-1}{3}+p)}$. This is impossible since $\frac{p^n-1}{3}+p\not\equiv 0 \pmod 3$.

Case VII. Assume $\varphi(x_1)=\omega$ and $\varphi(x_2)=\omega^2$. In this case, $f(x_1)=f(x_2)$ implies $x_1^3=x_2^p$. Then we can deduce to $1=(x_1^3)^{\frac{p^n-1}{3}}=(x_2^p)^{\frac{p^n-1}{3}}=\omega^{2p}$. This is impossible since $p\not\equiv 0 \pmod 3$. □

Replacing the item x^3 by x^{p^i}, we get the following theorem. The proof is similar as in the proof of Theorem 9 and we omit it here.

Theorem 10. *Let i be any positive integer and assume $p^n\equiv 1 \pmod 9$. Then*

$$x\big(x^{\frac{p^n-1}{3}}-\omega\big)\big(x^{\frac{p^n-1}{3}}-\omega^2\big)+x^{p^i}\big(x^{\frac{p^n-1}{3}}-1\big)\big(x^{\frac{p^n-1}{3}}-\omega^2\big)+\omega x^p\big(x^{\frac{p^n-1}{3}}-1\big)\big(x^{\frac{p^n-1}{3}}-\omega\big)$$

is a PP over $\mathbb{F}_{p^n}$ if

(i) $p\equiv 1 \pmod 3$; *or*
(ii) *i is odd, $p\equiv 2 \pmod 3$.*

Theorems 9 and 10 present a new method to construct PPs. Using piecewise functions, we can get many different PPs which are combined with items x^3 and x^{p^i} $(0\leqslant i\leqslant n-1)$. For example, if n is even and $2^n\equiv 4 \pmod 9$, or equivalently, if $n\equiv 2 \pmod 6$,

$$g(x)=\big(x+x^2\big)x^{\frac{2^n-1}{3}}+x+\omega x^2+\big(x^{\frac{2^n-1}{3}}+1\big)\big(x^{\frac{2^n-1}{3}}+\omega\big)\big(x+\omega^2x^2+x^3\big)$$

is a PP over $\mathbb{F}_{2^n}$, which has the following piecewise function expression

$$g(x)=\begin{cases}0, & \text{if } x=0,\\ \omega^2x^2, & \text{if } \varphi(x)=1,\\ \omega^2x, & \text{if } \varphi(x)=\omega,\\ \omega x^3, & \text{if } \varphi(x)=\omega^2.\end{cases}$$

The following theorem uses multiplicative characters of finite fields of order t.

Theorem 11. *Assume $p\equiv 1 \pmod t$ and $p^n\equiv 1 \pmod{t^2}$ and let θ be an element of $\mathbb{F}_{p^n}$ of order t. Then*

$$f(x)=\sum_{i=1}^{t}x^{p^i}\prod_{j=1,\,j\neq i}^{t}\big(x^{(p^n-1)/t}-\theta^j\big)$$

is a PP over $\mathbb{F}_{p^n}$.

Proof. Let β be a primitive element of $\mathbb{F}_{p^n}$ such that $\theta = \beta^{(p^n-1)/t}$. Clearly, $f(0) = 0$. For nonzero $x \in \mathbb{F}_{p^n}$, $\pi(x) := x^{(p^n-1)/t}$ must be a power of θ, and let $\pi(x) = \theta^i$, $1 \leqslant i \leqslant t$, then we get

$$\begin{aligned} f(x) &= \left(\theta^i - \theta\right)\left(\theta^i - \theta^2\right)\cdots\left(\theta^i - \theta^{i-1}\right)\left(\theta^i - \theta^{i+1}\right)\cdots\left(\theta^i - \theta^t\right)x^{p^i} \\ &= \theta^{(t-1)i}(1-\theta)\cdots\left(1-\theta^{t-1}\right)x^{p^i} \neq 0. \end{aligned}$$

If $f(x_1) = f(x_2)$ and $\pi(x_1) = \pi(x_2) = \theta^i$ for some $1 \leqslant i \leqslant t$. Then $x_1^{p^i} = x_2^{p^i}$, which leads to $x_1 = x_2$.

Now we assume that $f(x_1) = f(x_2)$, $\pi(x_1) = \theta^i$, $\pi(x_2) = \theta^j$ for $1 \leqslant i \neq j \leqslant t$. Then we get

$$\theta^{(t-1)i} x_1^{p^i} = \theta^{(t-1)j} x_2^{p^j}. \tag{10}$$

Since $\frac{p^n-1}{t} \equiv 0 \pmod{t}$, we get $\theta^{(p^n-1)/t} = 1$. Taking Eq. (10) to the $\frac{p^n-1}{t}$th powers we obtain $\pi(x_1)^{p^i} = \pi(x_2)^{p^j}$, i.e., $\theta^{ip^i} = \theta^{jp^j}$. Since $p \equiv 1 \pmod{t}$, which contradicts to the assumption $1 \leqslant i \neq j \leqslant t$. Thus, we get that $f(x)$ is a PP over $\mathbb{F}_{p^n}$. □

Acknowledgments

The authors would like to thank the reviewers for their detailed comments that improved the quality and presentation of this paper. This work was supported by the National Basic Research Program of China (2007CB311201) and the National Natural Science Foundation of China (61070172, 10990011 and 11071107).

References

[1] A. Akbary, D. Ghioca, Q. Wang, On constructing permutations of finite fields, Finite Fields Appl. 17 (1) (2011) 51–67.
[2] X. Cao, L. Hu, New methods for generating permutation polynomials over finite fields, Finite Fields Appl. 17 (6) (2011) 493–503.
[3] P. Charpin, G. Kyureghyan, When does $G(X) + \gamma \operatorname{Tr}(H(X))$ permute $GF(p^n)$, Finite Fields Appl. 15 (5) (2009) 615–632.
[4] S.D. Cohen, Permutation group theory and permutation polynomials, in: Algebra and Combinatorics, Hong Kong, 1997, Springer, Singapore, 1999, pp. 133–146.
[5] C. Ding, Q. Xiang, J. Yuan, P. Yuan, Explicit classes of permutation polynomials of $\mathbb{F}_{3^{3m}}$, Sci. China Ser. A: Math. 53 (4) (2009) 639–647.
[6] T. Helleseth, V. Zinoviev, New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all m, Finite Fields Appl. 9 (2) (2003) 187–193.
[7] H.D.L. Hollmann, Q. Xiang, A class of permutation polynomials of $\mathbb{F}_{2^m}$ related to Dickson polynomials, Finite Fields Appl. 11 (1) (2005) 111–122.
[8] X. Hou, Two classes of permutation polynomials over finite fields, J. Combin. Theory Ser. A 118 (2) (2011) 448–454.
[9] X. Hou, G.L. Mullen, J.A. Sellers, J.L. Yucas, Reversed Dickson polynomials over finite fields, Finite Fields Appl. 15 (6) (2009) 748–773.
[10] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields Appl. 13 (1) (2007) 58–70.
[11] R. Lidl, H. Niederreiter, Finite Fields, 2nd ed., Encyclopedia Math. Appl., vol. 20, Cambridge University Press, 1997.
[12] G.L. Mullen, Permutation polynomials over finite fields, in: Proc. Conf. Finite Fields and Their Applications, in: Lect. Notes Pure Appl. Math., vol. 141, Marcel Dekker, New York, 1993, pp. 131–151.
[13] J. Yuan, C. Ding, Four classes of permutation polynomials of $\mathbb{F}_{2^m}$, Finite Fields Appl. 13 (4) (2007) 869–876.
[14] J. Yuan, C. Ding, H. Wang, J. Pieprzyk, Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$, Finite Fields Appl. 14 (2) (2008) 482–493.
[15] P. Yuan, C. Ding, Permutation polynomials over finite fields from a powerful lemma, Finite Fields Appl. 17 (6) (2011) 560–574.
[16] X. Zeng, X. Zhu, L. Hu, Two new permutation polynomials with the form $(x^{2^k} + x + \delta)^s + x$ over $\mathbb{F}_{2^n}$, Appl. Algebra Engrg. Comm. Comput. 21 (2) (2010) 145–150.